

Ficha técnica de licencia de software de ofimática

Gama 3 Nube	O365 E1 + Defender 365 P1 + Office 365 DtLP
Capacidad Unidad de almacenamiento de archivos (GB)	1.000 de almacenamiento personal en la nube
Capacidad Unidad de almacenamiento de correos (GB)	Buzón de 50 GB y mensajes de hasta 150 MB
¿Requiere licencia CAL? (*)	No requiere CAL Incluye CAL de Exchange Server Standard, Skype for Business Standard y SharePoint Server Standard.
Límite de Usuarios	Usuarios ilimitados
Informes y Auditoría Web	SI
Antiphishing y Antispam	SI

(*) Si es necesario una licencia adicional (CAL) esta debe estar incluida en el precio

1) Herramientas de Ofimática incluidas

- Correo electrónico: Incluye Exchange Online Plan 1 que contiene Buzón de 50 GB y mensajes de hasta 150 MB, además proteger la información mediante funcionalidades avanzadas. Los filtros antimalware y contra correo no deseado protegen los buzones.

Más información en este [link](#).

- Procesador de textos: Incluye Office for Web para abrir documentos de Word, Excel, OneNote y PowerPoint en el explorador web. Office para la Web facilita el trabajo y el uso compartido de archivos de Office desde cualquier lugar con una conexión a Internet, desde casi cualquier dispositivo a través de un navegador web. Los clientes de Microsoft 365 con Word, Excel, OneNote o PowerPoint pueden ver, crear y editar archivos en cualquier lugar.

Más información en este [link](#).

- Hoja de cálculos o planilla de cálculos: Incluye Office con Excel Online en el explorador web con funcionalidades para crear planillas de cálculo, crear tablas, utilizar funciones, agrupar datos, ocultar/mostrar filas, columnas y hojas, insertar gráficos, aplicar formato condicional, entre varias otras funcionalidades.

Más información en este [link](#).

- Programa de presentación: Incluye Office for Web para presentaciones incluye PowerPoint Online en el explorador web con funcionalidades como aplicación de temas y variaciones de temas, crear y administrar diapositivas, descarga y formato de fuentes, hipervínculos, insertar videos en línea, recortar imágenes, herramienta de corrección, coautoría en tiempo real, ejecutar presentaciones de diapositivas, entre otras funcionalidades.

Más información en este [link](#).

- Gestor de contactos: Incluye Exchange Online Plan 1 que contiene gestión de contactos y grupos disponible en el explorador web.

Más información en este [link](#).

- Gestor de información personal:
- Agenda o Calendario: Incluye Exchange Online Plan 1 que contiene calendario disponible en el explorador web a través de Outlook Online.

Más información en este [link](#).

- Herramientas colaborativas: Incluye Office for Web para abrir documentos de Word, Excel, OneNote y PowerPoint en el explorador web de forma colaborativa con otros usuarios para el uso compartido de archivos de Office desde cualquier lugar con una conexión a Internet, desde casi cualquier dispositivo a través de un navegador web. Los clientes de Microsoft 365 con Word, Excel, One Note o PowerPoint pueden ver, crear y editar archivos en cualquier lugar con herramientas de coautoría.

- Office para dispositivos móviles: Obtén las aplicaciones de Office para dispositivos iOS, Android y Windows con tamaños de pantalla de 10.1" o inferiores. Cada usuario puede instalar Office para dispositivos celulares en un máximo de cinco tabletas y cinco teléfonos. No se incluyen las aplicaciones de escritorio de Office.
- Outlook en la Web y para dispositivos celulares: Conéctate y permanece organizado con el correo, el calendario y los contactos en un solo lugar.
- Office Delve: Administra tu perfil de Office 365 con Delve. También puedes descubrir y organizar la información más importante para ti al instante y en todas tus aplicaciones de Office.
- Microsoft Bookings: Simplifica la forma en la que los clientes programan y administran las citas.
- Microsoft Whiteboard: Colabora con ideas y contenido con un lienzo digital de forma libre, que ahora está integrado en Microsoft Teams.
- SharePoint Online (plan 1): Comparte y administra tu contenido, así como tu información y tus aplicaciones, con 1 TB de almacenamiento de OneDrive por usuario. Impulsa el trabajo en equipo, encuentra información rápidamente y colabora con todos los miembros de la organización sin problemas.
- Microsoft OneDrive para el trabajo: Obtén acceso a 1 TB de almacenamiento personal en la nube, desde cualquier lugar y en cualquier dispositivo. Comparte archivos fácilmente con otros usuarios dentro y fuera de tu organización, y controla quién puede ver y editar cada archivo.
- Microsoft Sway: Crea boletines, presentaciones y documentaciones visualmente atractivos en cuestión de minutos.
- Microsoft Forms: Crea encuestas, cuestionarios y sondeos fácilmente.
- Microsoft Planner: Organiza el trabajo en equipo, crea planes, asigna tareas, comparte archivos, chatea y recibe actualizaciones sobre el progreso.

- Microsoft Graph: Usa este modelo de programación unificado para acceder a datos para crear aplicaciones para organizaciones y consumidores que interactúen con millones de usuarios.
- Office en la Web: Usa Outlook, Word, Excel, PowerPoint y OneNote para crear y compartir contenido, así como para colaborar en él, estés donde estés.
- Microsoft Teams: Participa en chats y reuniones, comparte archivos y usa aplicaciones empresariales en un área de trabajo compartida.
- Grupos de Office 365: Usa este servicio, junto con herramientas de Office 365 que ya usas, para colaborar con compañeros de trabajo al escribir documentos, crear hojas de cálculo, trabajar en planes de proyectos, programar reuniones o enviar correos.
- Viva Engage: Conecta con la red social empresarial e interactúa.
- Microsoft Stream: Carga, organiza y comparte contenido de video inteligente para toda la empresa.
- Power Apps para Microsoft 365: Crea las aplicaciones empresariales que necesitas y amplía o personaliza las que ya usas, la versión incluida es limitada con respecto a la versión full al no incluir conectores Premium, entre otras funcionalidades.
- Power Automate para Microsoft 365: Realiza tareas repetitivas con facilidad con la automatización de flujos de trabajo, la versión incluida es limitada con respecto a la versión full al no incluir conectores Premium, entre otras funcionalidades.
- Microsoft To Do: Planea tu día y administra tu vida.

Más información en este [link](#).

*Las características de los productos pueden experimentar cambios en su nombre o funcionalidades, dichas modificaciones pueden ser integradas en nuevas soluciones que podrían incluirse en las suite que se están adquiriendo.

2) Seguridad Estándar y herramientas de administración Estándar

El Centro de administración de Microsoft 365 permite gestionar los usuarios y aplicaciones de forma rápida y simple, en este portal se pueden agregar o eliminar a los usuarios y asignarle/desasignarle las licencias correspondientes, este portal tiene dos vistas: la vista simplificada ayuda a las organizaciones más pequeñas a administrar sus tareas más comunes. La vista panel incluye tareas y configuraciones más complejas. Puede cambiar entre ellos desde un botón en la parte superior del centro de administración.

En el Centro de administración de Microsoft 365, puede restablecer contraseñas, ver la factura, agregar o quitar usuarios y mucho más en un solo lugar.

Las áreas de trabajo especializadas, como seguridad o administración de dispositivos, permiten un control más pormenorizado y pueden descargar reportes de uso u obtener recomendaciones de seguridad presentes en la plataforma a través de una puntuación en el panel Secure Score.

Seguir las recomendaciones de la puntuación de seguridad puede proteger a su organización de amenazas

La puntuación de seguridad ayuda a las organizaciones a:

- Informar sobre el estado actual de la situación en materia de seguridad de la organización.
- Mejorar la situación de seguridad proporcionando capacidad de descubrimiento, visibilidad, orientación y control.
- Comparar con puntos de referencia y establecer indicadores clave de rendimiento (KPI).

De forma predeterminada, la persona que se registra y compra una suscripción de Microsoft 365 para empresas obtiene permisos de administrador. Esa persona puede asignar permisos de administrador a otras personas para ayudarles a administrar Microsoft 365 para su organización.

*Para poder descargar estos reportes se requiere el rol adecuado dentro del portal de administración, el cual se gestiona a nivel interno en la organización.

Más información en este [link](#).

3) Seguridad Avanzada y herramientas de administración móviles

Microsoft Defender para Office 365 es una suite unificada de defensa empresarial previa y posterior a la violación que coordina de forma nativa la detección, la prevención, la investigación y la respuesta en los puntos finales, las identidades, el correo electrónico y las aplicaciones para proporcionar una protección integrada contra los ataques sofisticados.

Archivos adjuntos seguros

Safe Attachments en Microsoft Defender para Office 365 proporciona una capa adicional de protección para los archivos adjuntos de correo electrónico que ya han sido analizados por la protección antimalware en Exchange Online Protection (EOP). En concreto, Safe Attachments utiliza un entorno virtual para comprobar los archivos adjuntos en los mensajes de correo electrónico antes de que se entreguen a los destinatarios (un proceso conocido como detonación).

Enlaces seguros

Vínculos seguros es una función de Defender para Office 365 que permite analizar y reescribir las URL de los mensajes de correo electrónico entrantes en el flujo de correo, así como verificar las URL y los vínculos de los mensajes de correo electrónico y otras ubicaciones al hacer clic en ellos. El análisis de Safe Links se produce además de la protección antispam y antimalware habitual en los mensajes de correo electrónico entrantes en Exchange Online Protection (EOP). El análisis de Safe Links puede ayudar a proteger a su organización de los enlaces maliciosos que se utilizan en el phishing y otros ataques.

Archivos adjuntos seguros para SharePoint, OneDrive y Microsoft Teams

Safe Attachments para SharePoint, OneDrive y Microsoft Teams en Microsoft Defender para Office 365 proporciona una capa adicional de protección para los archivos que ya han sido analizados en el momento de la carga por el motor de detección de virus común en Microsoft 365. Safe Attachments for SharePoint, OneDrive y Microsoft Teams ayuda a detectar y bloquear los archivos

existentes que se identifican como maliciosos en los sitios de equipo y las bibliotecas de documentos.

Protección antiphishing en Defender para Office 365

La política antiphishing predeterminada de Microsoft Defender para Office 365 proporciona protección contra la suplantación de identidad e inteligencia de buzón para todos los destinatarios.

Detecciones en tiempo real

El explorador o las detecciones en tiempo real ayudan a su equipo de operaciones de seguridad a investigar y responder a las amenazas de manera eficiente.

[Link](#)

4) DLP

Microsoft Data Loss Prevention (DLP, por sus siglas en inglés) tiene el objetivo de identificar, monitorear y proteger automáticamente la información confidencial en Office 365.

Implementando una política de DLP se puede lograr:

- Identificar información confidencial en muchas ubicaciones, como Exchange Online, SharePoint Online, OneDrive para empresas y Microsoft Teams.
- Evitar el intercambio accidental de información confidencial.
- Supervisar y proteger la información confidencial en las versiones de escritorio de Excel, PowerPoint y Word.
- Ayudar a los usuarios a aprender cómo cumplir con las normas sin interrumpir su flujo de trabajo.
- Ver alertas e informes de DLP que muestran contenido que coincide con las políticas de DLP de su organización.

[Link](#)

5) Identidad Avanzada

El portal de administración permite la descarga de reportes de uso del licenciamiento de los usuarios, adicionalmente al usar esta plataforma se incluyen las siguientes funcionalidades de Multifactor de autenticación presentes en Office 365.

Característica	Office 365
Protección de cuentas de administración de inquilinos de Entra ID con MFA	●
Aplicación móvil como segundo factor	●
Llamada de teléfono como segundo factor	●
SMS como segundo factor	●
Control administrativo sobre métodos de comprobación	●
Recordar MFA para dispositivos de confianza	●

Más información en este [link](#).

6) Informes y Auditoria Móvil

El portal de administración de Office 365 se puede gestionar fácilmente el uso que hacen de los servicios de Microsoft 365 los usuarios de la organización a través de informes detallados sobre el uso del correo electrónico, OneDrive, SharePoint, Yammer y Microsoft Teams para los últimos 7, 30, 90 o 180 días. Los datos no estarán disponibles para todos los períodos de informes al instante. Los informes están disponibles en 48 horas.

*Para poder descargar estos reportes se requiere el rol adecuado dentro del portal de administración, el cual se gestiona a nivel interno en la organización.

Más información en este [link](#).

7) Requisitos de instalación y/o uso

Contactar al proveedor adjudicado para instrucciones.

Requisitos técnicos

Procesador necesario	Windows: 1.6 gigahercios (GHz) o más rápido, dos núcleos macOS: Procesador Intel
Sistema operativo necesario	Windows: Windows 11, Windows 10 SAC, Windows 8.1, Windows Server 2019 o Windows Server 2016. Ten en cuenta que Aplicaciones Microsoft 365 para empresas no es compatible con ningún producto cliente de Windows 10 LTSC. Aplicaciones Microsoft 365 para empresas es compatible con Windows Server 2019 en Windows Server 2016 hasta octubre de 2025. macOS: Office para Mac es compatible con las tres versiones más recientes de macOS. Cuando se publica una nueva versión de macOS, el requisito del sistema operativo de Office para Mac es tener las tres versiones más recientes en ese momento: la nueva versión de macOS y las anteriores. La disponibilidad de funciones y características del producto puede variar en sistemas anteriores. Para disfrutar de la mejor experiencia, usa la versión más reciente de cualquier sistema operativo especificado anteriormente.
Memoria necesaria	Windows: 4 GB de RAM; 2 GB de RAM (32 bits) macOS: 4 GB de RAM
Espacio en disco duro necesario	Windows: 4 GB de espacio disponible en disco macOS: 10 GB de espacio disponible en disco. Disco duro con formato HFS+ (también conocido como macOS Extended o APFS)
Pantalla necesaria	Windows: Resolución de pantalla de 1280 × 768 macOS: Resolución de pantalla de 1280 × 800

Gráficos	Windows: La aceleración de hardware de gráficos necesita DirectX 9 o versiones posteriores, con WDDM 2.0 o posteriores para Windows 10 (o bien WDDM 1.3 o posteriores para Windows 10 Fall Creators Update). macOS: Sin requisitos de gráficos
Multitáctil	Se necesita un dispositivo táctil para usar las funciones multitáctiles. Pero todas las características y funciones siempre estarán disponibles mediante el teclado, el mouse o cualquier otro dispositivo de entrada accesible o estándar. Las características táctiles están optimizadas para su uso con Windows 10 o Windows 8.1.
Requisitos del sistema adicionales	Las funciones y los gráficos del producto pueden variar según la configuración del sistema. Para usar algunas de las características, puede que se necesite hardware adicional o avanzado, o bien conectividad de servidor. Se necesita una cuenta Microsoft o una cuenta de organización para la asignación de licencias y el acceso a los servicios. Para usar la funcionalidad de Internet, se necesita una conexión a Internet.

8) Consola

Desde la consola se pueden generar políticas de conservación local y retención por juicio, al colocar un buzón en Conservación local o retención por juicio, la conservación o retención se aplica al buzón principal y al buzón de archivo.

Estas funcionalidades se administran desde el portal de cumplimiento Microsoft Purview para habilitar buzones de archivo en pos de admitir los requisitos de retención de mensajes, exhibición de documentos electrónicos y retención de mensajes de la organización, adicionalmente puede crear una directiva de archivado y eliminación en Microsoft 365 que mueva automáticamente los elementos al buzón de archivo de un usuario.

Sobre el cifrado de la información en el correo electrónico, Microsoft usa seguridad de la capa de transporte (TLS) y secreto de reenvío (FS) para proteger las comunicaciones.

TLS (Seguridad de la capa de transporte) y SSL (antecesor de TLS) son protocolos criptográficos que protegen la comunicación por red con certificados de seguridad que cifran una conexión entre equipos. TLS reemplaza a Capa de sockets seguros (SSL) y a menudo se conoce como SSL 3.1. Exchange Online usa TLS para cifrar las conexiones entre los servidores de Exchange y las conexiones entre los servidores de Exchange y otros servidores, como los servidores de Exchange locales o los servidores de correo de los destinatarios. Una vez cifrada la conexión, todos los datos enviados a través de esa conexión se envían a través del canal cifrado. Sin embargo, si reenvía un mensaje que se envió a través de una conexión cifrada con TLS a una organización de destinatarios que no admite el cifrado TLS, ese mensaje no se cifra necesariamente.

Use TLS en situaciones en las que quiera configurar un canal seguro de correspondencia entre Microsoft y su organización local u otra organización, como un asociado. Exchange Online siempre intenta usar TLS primero para proteger el correo electrónico, pero no puede hacerlo si la otra parte no ofrece seguridad TLS.

En cuanto al cifrado de la información confidencial en sus centros de datos, Microsoft utiliza una tecnología denominada Distributed Key Manager, esta es una funcionalidad del lado cliente que usa un conjunto de claves secretas para cifrar y descifrar información. Solo los miembros de un grupo de seguridad específico de los Servicios de dominio de Active Directory pueden tener acceso a dichas claves para descifrar los datos cifrados por el DKM. En Exchange Online, solo determinadas cuentas de servicio bajo las cuales se ejecutan procesos de Exchange forman parte del grupo de seguridad. Como parte del procedimiento operativo estándar en el centro de datos, ningún humano tiene credenciales que forman parte de este grupo de seguridad y, por lo tanto, nadie tiene acceso a las claves que pueden descifrar la información confidencial.

Para depuración, solución de problemas o fines de auditoría, un administrador del centro de datos debe solicitar acceso con privilegios elevados para obtener credenciales temporales que forman parte del grupo de seguridad. Este proceso requiere varios niveles de aprobación legal. Si se concede acceso, toda la actividad se registra y se audita. Además, solo se otorga acceso durante un determinado intervalo de tiempo, que caduca automáticamente una vez concluido.

Para brindar protección adicional, la tecnología del DKM incluye sustitución de claves y archivado automático. Esto también garantiza el acceso al contenido anterior sin tener que recurrir a la misma clave de forma indefinida.

En cuanto a la gestión de políticas de Grupo y políticas en la nube, la consola en el centro de administración de Aplicaciones Microsoft 365 permite aplicar la configuración de directivas para Aplicaciones Microsoft 365 para empresas en el dispositivo de un usuario, incluso si el dispositivo no está unido a un dominio o administrado de otro modo. Cuando un usuario inicia sesión en las Aplicaciones de Microsoft 365 para empresas en un dispositivo, la configuración de la Directiva se desplaza a ese dispositivo. La configuración de directivas está disponible para dispositivos con Windows, macOS, iOS y Android, aunque no todas las opciones de configuración de directiva están disponibles para todos los sistemas operativos. También puede aplicar algunas configuraciones de directiva para Office para la Web, tanto para los usuarios que han iniciado sesión como para los usuarios que tienen acceso a documentos de forma anónima.

La directiva de nube admite grupos de seguridad y grupos de seguridad habilitados para correo creados o sincronizados con Azure AD.

Al crear configuraciones de directiva, puede revisar y aplicar las directivas recomendadas por Microsoft como directivas de línea base de seguridad. Estas recomendaciones se marcan como "Línea base de seguridad" al seleccionar directivas.

Más información sobre Archiving en este [link](#), en cuanto al cifrado de la información en la capa de transporte en este [link](#), sobre la protección de los datos en almacenamiento en este [link](#) y sobre políticas de directivas en este [link](#).

*Para crear una configuración de directiva, debe tener asignado el rol adecuado dentro del portal de administración, el cual se gestiona a nivel interno en la organización.

9) Otra información relevante del producto

Los productos presentes cumplen con los más altos estándares y corresponden a soluciones de nivel global que se comercializan con una elevada calidad empresarial, las funcionalidades descritas están enfocadas en cumplir los estándares solicitados por Mercado Publico a través de la licitación presente.